BY ORDER OF THE COMMANDER

SMC Tailoring SMC-T-004
30 November 2012

Supersedes:
New issue

Air Force Space Command

SPACE AND MISSILE SYSTEMS CENTER TAILORING

TAILORING INSTRUCTIONS FOR MIL-STD-882E

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
30 NOV 2012	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
SMC-T-004 (2012) Tailoring Instructions for MIL-STD-882E	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **USAF Space and Missile Systems Center**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**18**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

FOREWORD

This tailoring document defines the Government's requirements and expectations for government and contractor performance in defense system acquisitions and technology development.

This new-issue SMC tailoring adds some System Safety practices useful for Air Force Space and Missile Systems to MIL-STD-882E, while removing nothing. This tailoring is intended to assist the user in following the pertinent requirements of policy implementation documents. For example, when defining USAF preventable mishaps, include all reportable mishaps, which includes losses of systems and their mission capability (particularly in space systems) in addition to other types of losses. This tailored standard applies to the entire life cycle of systems, which for space systems includes pre-launch, launch and on-orbit including disposal. Apply this tailoring in coordination with other functional areas taking advantage of the Systems Engineering process to ensure affordable and robust systems.

Beneficial comments (recommendations, changes, additions, deletions, etc.) and any pertinent data that may be of use in improving this document should be forwarded to the following addressee using the "SMC Standard Improvement Proposal" Form appearing at the end of this document or by letter:

Division Chief, SMC/SES
SPACE AND MISSILE SYSTEMS CENTER
Air Force Space Command
482 N. Aviation Blvd.
El Segundo, CA 90245

This tailoring document has been approved for use on all Space and Missile Systems Center/ Air Force Program Executive Office – Space development, acquisition, and sustainment contracts.

Paul Mejasich, GG-15, DAFC, SMC/SE
SMC Director of Safety

Originated by: Francis G. McDougall
FRANCIS G. MCDOUGALL, GG-13, DAFC, SMC/SES

Coordinated by: Thomas C. Meyers
THOMAS C. MEYERS, GG-14, DAFC, SMC/SES
SMC Center System Safety Manager

1. Scope

1.1 Purpose

This document shall be used for tailoring MIL-STD-882E dated 11 May 2012, and provides a contractual Compliance Document listing that cites MIL-STD-882E and an annex with tailoring instructions.

1.2 Application

This document is intended for use in acquisition contracts for space systems and shall be cited in the contract Statement of Work (SOW) to specify the system safety requirements that are applicable to the acquisition of space systems or space system of systems (SoS) which may include space vehicles, upper-stage vehicles, injection stages, satellite payloads, reentry vehicles, launch vehicles or ballistic vehicles, ground control systems and user equipment systems.

2. Compliance Document and SMC Tailoring

The following section shows an example Compliance Document List entry for MIL-STD-882E indicating that tailoring is to be applied as described in the annex below. Portions of the MIL-STD-882E that do not need SMC tailoring have been incorporated by reference.

2.1 Core Compliance Document

Document Number	Title	Pub Date
MIL-STD-882E	System Safety	11 May 2012

2.2 Reference Documents

Additional information on System and Software Safety related Tasks are available from the documents listed below.

a. *Joint Software Systems Safety Engineering Handbook,* Naval Ordnance Safety and Security Activity, Version 1.0, 27 August 2010.

b. GEIA/ANSI-STD-0010, *Standard Best Practices for System Safety Program Development and Execution,* Tech America, 12 February 2009.

c. AOP-52 (EDITION 1), *Guidance On Software Safety Design And Assessment Of Munition-Related Computing Systems* (NATO), 9 December 2008.

d. AFI 63-101, *Acquisition and Sustainment Life Cycle Management.*

e. AFI 63-1201, *Assurance of Operational Safety, Suitability, & Effectiveness.*

f. AFI 91-202, *The US Air Force Mishap Prevention Program.*

g. AFI 91-202_AFSPCSUP_I, *The US Air Force Mishap Prevention Program.*

h. AFI 91-204, *Safety Investigations and Reports.*

i. AFI 91-204_AFSPCSUP_I, *Safety Investigations and Reports.*

j. AFI 91-217, *Space Safety and Mishap Prevention Program.*

k. AFMAN 91-222, *Space Safety Investigations and Reports.*

l. AFSPCMAN 91-710, *Range Safety User Requirements Manual – Range Safety Policies and Procedures.*

m. EWR 127-1, *Eastern and Western Ranges Requirements Manual.*

n. RCC-319, *Range Commanders Council Flight Termination Systems Commonality Standard.*

o. RCC-321, *Range Commanders Council Common Risk Criteria For National Test Ranges.*

p. SMCI 63-1205, *The SMC System Safety Program.*

q. SMCI 63-1207 (Draft), *Programmatic Environmental, Safety & Occupational Health Evaluation.*

2.3 Tailoring Annex

The following section describes the SMC tailoring for MIL-STD-882E, *System Safety*. The numbering in the tailoring below are the paragraph numbers from MIL-STD-882E.

The U.S. Government requirements for Standard Practice For System Safety are contained in the Department of Defense Instruction (DoDI), DoDI 5000.02, *Operation of the Defense Acquisition System;* Air Force Instructions (AFI), AFI 63-101, *Acquisition And Sustainment Life Cycle Management;* AFI 63-1201, *Life Cycle Systems Engineering;* and AFI 91-202 including its AFSPC Supplement, AFI 91-202_AFSPCSUP_I, both titled *The US Air Force Mishap Prevention Program;* which are the source authorities for the derived requirements for systems acquisition for the Air Force, Air Force Space Command (AFSPC), and the SMC. References to these requirements are also found in SMCI 63-1205, *The SMC System Safety Program*.

1. SCOPE

1.1. Add, “This SMC-tailored MIL-STD outlines the SMC standard practice for conducting system safety. The system safety practice as defined herein conforms to DoDI 5000.02, AFI 63-101, AFI 63-1201, AFI 91-202 AFSPC Sup 1 and SMCI 63-1205 and provides a consistent

means of evaluating identified risks. Mishap risk must be identified, evaluated, and mitigated to a level acceptable (as defined by risk acceptance authorities, the system user or customer) to the appropriate authority and compliant with federal (and state and local where applicable) laws and regulations, Executive Orders, policies, treaties, and agreements. Program trade studies associated with mitigating mishap risk must consider total life cycle cost in any decision."

2. APPLICABLE DOCUMENTS

2.1 There are no changes to this paragraph—use MIL-STD-882E verbatim.

2.2.1 There are no changes to this paragraph—use MIL-STD-882E verbatim.

2.2.2 There are no changes to this paragraph—use MIL-STD-882E verbatim.

2.3 There are no changes to this paragraph—use MIL-STD-882E verbatim.

3. DEFINITIONS

3.1 Acronyms.

Add: "AFI - Air Force Instruction
AFMAN – Air Force Manual
AFSPCI – Air Force Space Command Instruction
AFSPCMAN - Air Force Space Command Manual
EWR – Eastern Western Range
RCC – Range Commanders Council
SMC - Space and Missile Systems Center
SMCI - SMC Instruction"

3.2 Definitions. There are no changes to this paragraph—use MIL-STD-882E verbatim.

3.2.1 Acceptable Risk. There are no changes to this paragraph—use MIL-STD-882E verbatim.

3.2.2 Acquisition program. There are no changes to this paragraph—use MIL-STD-882E verbatim.

3.2.3 Causal factor. There are no changes to this paragraph—use MIL-STD-882E verbatim.

3.2.4 Commercial-off-the-shelf (COTS). There are no changes to this paragraph—use MIL-STD-882E verbatim.

3.2.5 Contractor. There are no changes to this paragraph—use MIL-STD-882E verbatim.

3.2.6 Environmental impact. There are no changes to this paragraph—use MIL-STD-882E verbatim.

3.2.7 ESOH. There are no changes to this paragraph—use MIL-STD-882E verbatim.

3.2.8 Event risk. There are no changes to this paragraph—use MIL-STD-882E verbatim.

3.2.9 Fielding. There are no changes to this paragraph—use MIL-STD-882E verbatim.

3.2.10 Firmware. There are no changes to this paragraph—use MIL-STD-882E verbatim.

3.2.11 Government-furnished equipment (GFE). There are no changes to this paragraph—use MIL-STD-882E verbatim.

3.2.12 Government-furnished information (GFI). There are no changes to this paragraph—use MIL-STD-882E verbatim.

3.2.13 Government-off-the-shelf (GOTS). There are no changes to this paragraph—use MIL-STD-882E verbatim.

3.2.14 Hazard. Add, "For this SMC tailoring mishap includes all other types of reportable mishaps including space mishaps."

3.2.15 Hazardous material (HAZMAT). There are no changes to this paragraph—use MIL-STD-882E verbatim.

3.2.16 Human systems integration (HSI). There are no changes to this paragraph—use MIL-STD-882E verbatim.

3.2.17 Initial risk. There are no changes to this paragraph—use MIL-STD-882E verbatim.

3.2.18 Level of rigor (LOR). There are no changes to this paragraph—use MIL-STD-882E verbatim.

3.2.19 Life-cycle. There are no changes to this paragraph—use MIL-STD-882E verbatim.

3.2.20 Mishap. Add, "For the purpose of this SMC tailoring, mishap includes all reportable mishaps, which in turn includes space mishaps. Space mishaps include such things as unintentional release of space debris, failure to execute end-of-life actions, and losses of systems or their mission capability."

3.2.21 Mitigation measure. There are no changes to this paragraph—use MIL-STD-882E verbatim.

3.2.22 Mode. There are no changes to this paragraph—use MIL-STD-882E verbatim.

3.2.23 Monetary Loss. There are no changes to this paragraph—use MIL-STD-882E verbatim.

3.2.24 Non-developmental item (NDI). There are no changes to this paragraph—use MIL-STD-882E verbatim.

3.2.25 Probability. There are no changes to this paragraph—use MIL-STD-882E verbatim.

3.2.26 Program Manager (PM). There are no changes to this paragraph—use MIL-STD-882E verbatim.

3.2.27 Re-use items. There are no changes to this paragraph—use MIL-STD-882E verbatim.

3.2.28 Risk. There are no changes to this paragraph—use MIL-STD-882E verbatim.

3.2.29 Risk level. There are no changes to this paragraph—use MIL-STD-882E verbatim.

3.2.30 Safety. Add, "For the USAF Safety includes freedom from loss of systems and their mission capability."

3.2.31 Safety-critical. There are no changes to this paragraph—use MIL-STD-882E verbatim.

3.2.32 Safety-critical function (SCF). There are no changes to this paragraph—use MIL-STD-882E verbatim.

3.2.33 Safety-critical item (SCI). There are no changes to this paragraph—use MIL-STD-882E verbatim.

3.2.34 Safety-related. There are no changes to this paragraph—use MIL-STD-882E verbatim.

3.2.35 Safety-significant. There are no changes to this paragraph—use MIL-STD-882E verbatim.

3.2.36 Severity. Add, "For the USAF Space enterprise include the magnitude of potential consequences such as loss of systems or their mission capability, or space mishaps."

3.2.37 Software. There are no changes to this paragraph—use MIL-STD-882E verbatim.

3.2.38 Software control category. There are no changes to this paragraph—use MIL-STD-882E verbatim.

3.2.39 Software re-use. There are no changes to this paragraph—use MIL-STD-882E verbatim.

3.2.40 Software system safety. There are no changes to this paragraph—use MIL-STD-882E verbatim.

3.2.41 System. There are no changes to this paragraph—use MIL-STD-882E verbatim.

3.2.42 System-of-systems (SoS). There are no changes to this paragraph—use MIL-STD-882E verbatim.

3.2.43 System safety. Add, "Further objectives beyond the minimum include optimizing mishap risk as low as reasonably practicable, finding efficiencies and helping optimize cost, schedule and performance."

3.2.44 System safety engineering. There are no changes to this paragraph—use MIL-STD-882E verbatim.

3.2.45 System safety management. There are no changes to this paragraph—use MIL-STD-882E verbatim.

3.2.46 System/subsystem specification. There are no changes to this paragraph—use MIL-STD-882E verbatim.

3.2.47 Systems engineering. There are no changes to this paragraph—use MIL-STD-882E verbatim.

3.2.48 Target risk. There are no changes to this paragraph—use MIL-STD-882E verbatim.

3.2.49 User representative. There are no changes to this paragraph—use MIL-STD-882E verbatim.

4. GENERAL REQUIREMENTS

4.1 General. There are no changes to this paragraph—use MIL-STD-882E verbatim.

4.2 System safety requirements. There are no changes to this paragraph—use MIL-STD-882E verbatim.

4.3 System safety process.

4.3.1b. Insert between "Examples include" and "Insensitive Munitions (IM) requirements", "Space Debris minimization and disposal requirements,"

4.3.3. b (1) Add, "As of the writing of this SMC tailoring of this Standard, Current USAF policy requires quantified probability and event consequence severity levels (AFI 91-202 AFSPCSup1 Section 11.2.3.1.) A translation table from safety to the 5X5 risk matrix, required for milestone and technical reviews, assumed compatibility with the MIL-STD-882D Mishap Risk Assessment Matrix. Probabilities and severities must be IAW current applicable policy for government organizations, and are per the contract for contractors. In accordance with current DOD, USAF and AFSPC policy, risk packages will use the risk matrix defined in MIL-STD-882E and associated probabilities in Table A-II. Any tailoring will be done with the coordination and approval of users, risk acceptance authorities, process owners and safety staffs IAW current policy. Contracts using previous versions of MIL-STD-

882 may continue using those versions for contract purposes; however, government risk reporting and new risk acceptance packages must be converted to the MIL-STD-882E matrix and definitions used IAW current policy."

4.3.3.d Add, "Relevant DOD Component policy documents include AFI 91-202_AFSPCSUP_I and AFI 63-101."

5. DETAILED REQUIREMENTS

5.1 Additional information. Add, "For this SMC tailoring Appendix C, D and E exist, and also contain optional information."

5.2 Tasks. There are no changes to this paragraph—use MIL-STD-882E verbatim.

5.3 Task structure. There are no changes to this section—use MIL-STD-882E verbatim.

6. NOTES

6.1 Intended use. There are no changes to this paragraph—use MIL-STD-882E verbatim.

6.2 Acquisition requirements. There are no changes to this section—use MIL-STD-882E verbatim.

6.3 Associated Data Item Descriptions (DIDs). Add, "DI-SAFT-81563, Accident/Incident Report."

6.4 Subject term (key word) listing. There are no changes to this section—use MIL-STD-882E verbatim.

6.5 Changes from previous issue. There are no changes to this section—use MIL-STD-882E verbatim.

TASK 101- HAZARD IDENTIFICATION AND MITIGATION EFFORT USING THE SYSTEM SAFETY METHODOLOGY. There are no changes to this Task—use MIL-STD-882E verbatim.

TASK 102 - SYSTEM SAFETY PROGRAM PLAN. There are no changes to this Task—use MIL-STD-882E verbatim.

TASK 103 - HAZARD MANAGEMENT PLAN. There are no changes to this Task—use MIL-STD-882E verbatim.

TASK 104 - SUPPORT OF GOVERNMENT REVIEWS/AUDITS. There are no changes to this Task—use MIL-STD-882E verbatim.

TASK 105 - INTEGRATED PRODUCT TEAM/WORKING GROUP SUPPORT. There are no changes to this Task—use MIL-STD-882E verbatim.

TASK 106 - HAZARD TRACKING SYSTEM. There are no changes to Tasks 106.1, 106.2, 106.2.1, 106.2.2 and 106.3 —use MIL-STD-882E verbatim.

Add the following Task 106.2.3:

"Task 106.2.3. The contractor shall document in the HTS the following items as a result of performing Task 208 (Functional Hazard Analysis):

a. List of safety-critical functions (SCFs), safety-critical item (SCIs), safety-related functions (SRFs), and safety-related items (SRIs) of the system.

b. Allocation and mapping/linking of SCFs, SCIs, SRFs, and SRIs to the system design architecture in terms of hardware, software, and human interfaces.

c. Execution of SCF, SCI, SRF, and SRI requirements for technical documentation, markings and related analyses.

d. List of life cycle Critical Safety Items and their related status and disposition."

TASK 107 - HAZARD MANAGEMENT PROGRESS REPORT. There are no changes to this Task—use MIL-STD-882E verbatim.

TASK 108 - HAZARDOUS MATERIALS MANAGEMENT PLAN. There are no changes to this Task—use MIL-STD-882E verbatim.

NOTE: The following Task 109 is an accredited and accepted requirement extracted from ANSI/GEIA-STD-0010, 12 February 2009,

Add the following Task 109 (ANSI/GEIA-STD-0010, 12 February 2009):

"Task 109 – Launch Safety Program Requirements

109.1 Purpose

The purpose of this task is to require the contractor to support special safety requirements specific to launch facilities including range design and operation.

109.2 Task Description

The contractor must comply with the following requirements, as tailored by the Program Manager (PM), when this task is called out in the contract.

109.2.1 Unacceptable/Acceptable Conditions

a. Unacceptable conditions. The following safety critical conditions are considered unacceptable. Positive action and implementation verification is required to reduce the risk to an acceptable level as negotiated by the contractor and the Program Manager (PM).

(1) Single component failure, common mode failure, human error, or design features that could result in mishaps as defined by the Program Manager (PM).

(2) Dual independent component failures, dual human errors, or a combination of a component failure and a human error involving safety critical command and control functions, which could result in mishaps as defined by the Program Manager (PM).

(3) Generation of hazardous ionizing/non-ionizing radiation or energy when no provisions have been made to protect personnel or sensitive subsystems from damage or adverse effects.

(4) Packaging or handling procedures and characteristics that could cause a mishap for which no controls have been provided to protect personnel or sensitive equipment.

(5) Hazard level categories that are specified as unacceptable in the contract.

b. Acceptable conditions. The following approaches are considered acceptable for correcting unacceptable conditions and will require no further analysis once controlling actions are implemented and verified.

(1) For non safety critical command and control functions; a system design that requires two or more independent human errors, or that requires two or more independent failures, or a combination of independent failure and human error.

(2) For safety critical command and control functions; a system design that requires at least three independent failures, or three human errors, or a combination of three independent failures and human errors.

(3) System designs that positively prevent errors in assembly, installation, or connections that could result in a mishap.

(4) System designs that positively prevent damage propagation from one component to another or prevent sufficient energy propagation to cause a mishap.

(5) System design limitations on operation, interaction, or sequencing that preclude occurrence of a mishap.

(6) System designs that provide an approved safety factor or fixed design allowance that limits, to an acceptable level, possibilities of structural failure or release of energy sufficient to cause a mishap.

(7) System designs that control energy build-up that could potentially cause a mishap (fuses, relief valves, electrical explosion proofing, etc.).

(8) System designs in which component failure can be temporarily tolerated because of residual strength or alternate operating paths so that operations can continue with a reduced but acceptable safety margin.

(9) System designs that positively alert the controlling personnel to a hazardous situation for which the capability for operator reaction has been provided.

(10) System designs that limit/control the use of hazardous materials.

109.2.2 Associate Safety Programs.

109.2.2.1 Industrial Safety and Hygiene

The contractor must conduct the system safety program so that it augments and supplements existing industrial safety and toxicology activities. This coordinated effort must assure that equipment or properties being used or developed under contract are protected from damage or mishap risk. When contractor owned or leased equipment is being used in manufacturing, testing, or handling of products developed or produced under contract, analysis and operational proof checks must be performed to show that risk of damage to those products has been minimized through proper design maintenance and operation by qualified personnel using approved procedures. This standard does not cover those functions that the contractor is required by law to perform under Federal or State OSHA, DOT, or EPA regulations.

109.2.2.2 Operational Site Safety

The contractor system safety program must encompass operational site activities. These activities must include all operations listed in the operational time lines, including system installation, checkout, modification, and operation. Particular attention must be given to operations and interfaces with ground support equipment and to the needs of the operators relating to personnel subsystems such as: panel layouts, individual operator tasks, fatigue prevention, biomedical considerations, etc.

109.2.2.3 Facilities

The contractor must include facilities in the system safety analyses activity. Facility safety design criteria must be incorporated in the facility specification. Consideration must be given to the test, operational, and maintenance aspects of the program. Identified requirements must include consideration of the compatibility with standards equal to or better than those specified by the most stringent of Federal, State, and Local Regulations. The test and operations safety procedures must encompass all development, qualification, acceptance tests, and operations. The procedures must include inputs from the safety analyses and must identify test, operations, facility, and support requirements. The procedures must be upgraded

and refined as required to correct deficiencies identified by the system safety analyses to incorporate additional safety requirements.

109.2.3 Range Safety

Compliance with the design and operational criteria contained in the applicable range safety manuals, regulations, and standards must be considered in the system safety analysis and the system safety criteria. System safety is concerned with minimizing risk to on- or off-site personnel and property arising from system operations on a range.

109.2.4 Drone and Missile System Safety

a. Verification of system design and operational planning compliance with range or operating site safety requirements must be documented in the SAR or as otherwise specified in the contract SOW and CDRL.

b. Ensure that flight analysis and flight termination systems comply with the requirements of the test range being utilized. Such requirements are applicable to the system during all flight phases until vehicle/payload impact or orbital insertion. The SAR or other safety report, as specified in the CDRL, must include all aspects of flight safety systems.

c. The contractor's system safety representatives will be an integral part of the flight evaluation and assessment team that reviews field/flight operations to correct any identified deficiencies and recommend appropriate safety enhancements during the field/flight operation process.

109.3 Details to be Specified

Details to be specified in the contract must include the following, as applicable:

(R) a. Imposition of Tasks 101 and 109.

(R) b. Identification of the paragraphs in Task 109 that apply or do not apply."

TASK 201 - PRELIMINARY HAZARD LIST. There are no changes to this Task—use MIL-STD-882E verbatim.

TASK 202 - PRELIMINARY HAZARD ANALYSIS. There are no changes to this Task—use MIL-STD-882E verbatim.

TASK 203 - SYSTEM REQUIREMENTS HAZARD ANALYSIS. There are no changes to this Task—use MIL-STD-882E verbatim.

TASK 204 - SUBSYSTEM HAZARD ANALYSIS. There are no changes to this Task—use MIL-STD-882E verbatim.

TASK 205 - SYSTEM HAZARD ANALYSIS. There are no changes to this Task—use MIL-STD-882E verbatim.

TASK 206 - OPERATING AND SUPPORT HAZARD ANALYSIS. There are no changes to this Task—use MIL-STD-882E verbatim.

TASK 207 - HEALTH HAZARD ANALYSIS. There are no changes to this Task—use MIL-STD-882E verbatim.

TASK 208 - FUNCTIONAL HAZARD ANALYSIS. There are no changes to this Task—use MIL-STD-882E verbatim.

TASK 209 - SYSTEM-OF-SYSTEMS HAZARD ANALYSIS. There are no changes to this Task—use MIL-STD-882E verbatim.

TASK 210 - ENVIRONMENTAL HAZARD ANALYSIS. There are no changes to this Task—use MIL-STD-882E verbatim.

TASK 301 - SAFETY ASSESSMENT REPORT. There are no changes to this Task—use MIL-STD-882E verbatim.

TASK 302 - HAZARD MANAGEMENT ASSESSMENT REPORT. There are no changes to this Task—use MIL-STD-882E verbatim.

TASK 303 - TEST AND EVALUATION PARTICIPATION. There are no changes to this Task—use MIL-STD-882E verbatim.

TASK 304 - REVIEW OF ENGINEERING CHANGE PROPOSALS, CHANGE NOTICES, DEFICIENCY REPORTS, MISHAPS, AND REQUESTS FOR DEVIATION/WAIVER. There are no changes to this Task—use MIL-STD-882E verbatim.

TASK 401 - SAFETY VERIFICATION. There are no changes to this Task—use MIL-STD-882E verbatim.

TASK 402 - EXPLOSIVES HAZARD CLASSIFICATION DATA. There are no changes to this Task—use MIL-STD-882E verbatim.

TASK 403 - EXPLOSIVE ORDNANCE DISPOSAL DATA. There are no changes to this Task—use MIL-STD-882E verbatim.

APPENDIX A - **GUIDANCE FOR THE SYSTEM SAFETY EFFORT.** There are no changes to this Task—use MIL-STD-882E verbatim.

APPENDIX B - **SOFTWARE SYSTEM SAFETY ENGINEERING AND ANALYSIS.**
There are no changes to this Task—use MIL-STD-882E verbatim.

Add the following Appendix C:

"APPENDIX C – **QUALIFICATIONS FOR KEY SYSTEM SAFETY PERSONNEL**
(Adapted from MIL-STD-882C).

Qualifications for key system safety personnel must include adequate education and training, experience and proven ability (through means such as certification) in order for each key person to fulfill his or her role. Examples are provided in Table C-I.

TABLE C-I. **MINIMUM QUALIFICATIONS FOR KEY SYSTEM SAFETY PERSONNEL.**

***Program Complexity And Hazard Potential	Education	Experience	Certification
High	*BS in Engineering, Physical Science, plus training in System Safety.	Four years in system safety.	Desired: Certified Safety Professional (CSP)** or Professional Engineer.
Moderate	Bachelor's Degree plus training in System Safety.	Two years in system safety or related discipline.	Enhancement: CSP or Professional Engineer.
Low	High School Diploma plus training in System Safety.	Four years in system safety.	Enhancement: CSP

*NOTE: Managing Authority May specify other degrees or certification in SOW.
**CSP – Certified Safety Professional.
***Practically all SMC programs are of high complexity and hazard potential."

Add the following Appendix D:

"APPENDIX D – UNACCEPTABLE/ACCEPTABLE CONDITIONS

This Appendix is not a mandatory part of the Standard. This Appendix is a starting point for

writing fault tolerance requirements that may be mandatory for some space-related systems (e.g., general range safety systems not covered by another requirement per AFMAN91-710, or safety catastrophic functions such as missile warning per AFI 91-217). For other particularly safety critical applications, the requirements of this Appendix are options to be considered by program managers and engineers. They are typically applied to command-and control type safety critical functions as the words below are from ANSI/GEIA-STD-0010-2009 Appendix A7.

A.7 Contract Terms and Conditions

Some acquisitions include the following conditions in their solicitation, system specification, or contract as requirements for the system design. These condition statements are used optionally as supplemental requirements based on specific program needs, and are worded below as they would appear if used in this manner.

A.7.1 Unacceptable Conditions

The following safety critical conditions are considered unacceptable for development efforts. Positive action and verified implementation is required to reduce the mishap risk associated with these situations to a level acceptable.

• Single component or multi-component single-point failure, common mode failure, human error, or a design feature that could result in a mishap of critical or catastrophic severity.

• Dual independent component failures, dual independent human errors, or a combination of a component failure and a human error involving safety critical command and control functions, which could result in a mishap of catastrophic severity.

• Generation of hazardous radiation or energy, when no provisions have been made to protect personnel or sensitive subsystems from damage or adverse effects.

• Packaging or handling procedures and characteristics that could cause a mishap for which no mitigators have been provided to protect personnel or sensitive equipment.

• Hazard categories that are specified as unacceptable in the development agreement.

• Component design or location that fails to address human physical, anthropometrics, physiological and/or perceptual-cognitive capabilities or limitations.

A.7.2 Acceptable Conditions

The following approaches are considered acceptable for correcting unacceptable conditions and will require no further analysis once mitigating actions are implemented and verified to an acceptance condition.

• For non-safety critical command and control functions: a system design that requires two or more independent human errors, or that requires two or more independent failures, or a combination of independent failure and human error.

• For safety critical command and control functions: a system design that requires at least three independent failures, or three independent human errors, or a combination of three independent failures and human errors.

• System designs that positively prevent errors in assembly, installation, or connections that could result in a mishap.

• System designs that positively prevent damage propagation from one component to another or prevent sufficient energy propagation to cause a mishap.

• System design limitations on operation, interaction, or sequencing that preclude occurrence of a mishap.

• System designs that provide an approved safety factor, or a fixed design allowance that limits, to an acceptable level, possibilities of structural failure or release of energy sufficient to cause a mishap.

• System designs that control energy build-up that could potentially cause a mishap (e.g., fuses, relief valves, or electrical explosion proofing).

• System designs where component failure can be temporarily tolerated because of residual strength or alternate operating paths, so that operations can continue with a reduced but acceptable safety margin. (When feasible, consider providing a warning indicator when a primary control system fails or the alternative control system is engaged).

• System designs that positively alert the controlling personnel to a hazardous situation where the capability for operator reaction can been provided.

• System designs that limit or control the use of hazardous materials."

Add the following Appendix E:

"APPENDIX E – ADDITIONAL GUIDANCE

For additional guidance on Total System Risk measures and criteria, development and tailoring of risk matrices, and optimally reducing safety risk as low as reasonably practicable (ALARP), ANSI/GEIA 0010-2009 is a good reference."

SMC Standard Improvement Proposal

INSTRUCTIONS

1. Complete blocks 1 through 7. All blocks must be completed.
2. Send to the Preparing Activity specified in block 8.

NOTE: Do not use this form to request copies of documents, or to request waivers, or clarification of requirements on current contracts. Comments submitted on this form do not constitute or imply authorization to waive any portion of the referenced document(s) or to amend contractual requirements. Comments submitted on this form do not constitute a commitment by the Preparing Activity to implement the suggestion; the Preparing Authority will coordinate a review of the comment and provide disposition to the comment submitter specified in Block 6.

SMC STANDARD CHANGE RECOMMENDATION:	**1. Document Number** SMC-T-004	**2. Document Date** 30 November 2012
3. Document Title	TAILORING INSTRUCTIONS FOR MIL-STD-882E	

4. Nature of Change
(Identify paragraph number; include proposed revision language and supporting data. Attach extra sheets as needed.)

5. Reason for Recommendation

6. Submitter Information

a. Name	**b. Organization**
c. Address	**d. Telephone**
e. E-mail address	**7. Date Submitted**

8. Preparing Activity

Space and Missile Systems Center
AIR FORCE SPACE COMMAND
483 N. Aviation Blvd.
El Segundo, CA 90245-2808
Attention: SMC/SES

March 2008